MAC0352 - Redes de Computadores e Sistemas Distribuídos
EP4

Prof. Daniel Macêdo Batista

1 Objetivo

O objetivo desta avaliação é permitir aos alunos explorar alguma vulnerabilidade em redes de computadores, mostrando qual a falha de programação que levou à vulnerabilidade e como essa falha pode ser corrigida.

Apesar de ser chamado de "EP", vocês não precisam escrever novos códigos. Utilizar códigos de exploits e patches existentes é recomendado mas é necessário que esses códigos sejam compreendidos para que possam ser explicados em sala de aula. Simplesmente usar o exploit e o patch como um *script kiddie* não é o objetivo deste trabalho.

2 Tarefas

1. Escolha alguém para fazer o trabalho junto. **O trabalho não pode ser feito individualmente.** Deve ser feito em dupla. Caso haja uma quantidade ímpar de alunos, 1 único grupo terá três pessoas.

2. Escolha um tópico para fazer o seu trabalho. Ou seja, pesquise no google ou em fóruns de segurança de redes de computadores[1] sobre vulnerabilidades que foram descobertas em serviços de redes **a partir de 2016 e que tenham soluções**. As vulnerabilidades podem ser em qualquer camada da arquitetura Internet.

3. Estude a vulnerabilidade, e sua solução, do ponto de vista de programação, e avalie se você conseguirá demonstrar em sala de aula. Caso você não consiga, volte para a Tarefa 2.

4. **Apresente o tópico para o professor no fim de alguma aula para ver a opinião dele**. Se ele disser que esse tópico é muito simples ou que não tem relação com redes de computadores, volte para a Tarefa 2. Tópicos enviados por email para o professor serão ignorados.

5. Escolha uma data para apresentar o seu trabalho e escreva na planilha disponível no PACA (já há uma thread sobre isso lá) as seguintes informações:

   Tópico; e

   Integrantes da equipe

[1] Recomendo que a busca seja feita em `https://cve.mitre.org/`

6. Prepare uma **apresentação de 25 minutos** em que você consiga explicar a falha, explorá-la ao vivo na sala de aula, aplicar a correção na falha, tentar explorá-la depois da correção e não conseguir, mostrando que a correção funcionou. Note que a explicação da falha tem que apresentar brevemente o serviço que você vai explorar, e mostrar, no código-fonte do serviço, onde está a falha. O patch que corrige o problema também precisa ser apresentado a nível de código-fonte. Recomenda-se fortemente que toda a demonstração da falha seja feita utilizando virtualização via `VirtualBox`, `Xen` ou `VMWare` e o `Wireshark`. **Tentativas de explorar serviços reais da USP ou de outro local serão punidas com nota ZERO na disciplina. Você deve apresentar a exploração em algum computador seu e em uma rede virtualizada durante a demonstração na sala de aula.**

As vulnerabilidades escolhidas para apresentar deverão ser a partir de 2016, mas **não** poderão ser as seguintes:

- CVE-2016-0800
- CVE-2016-4971
- CVE-2016-10033
- CVE-2016-10045
- CVE-2017-5638
- CVE-2017-8917
- CVE-2017-9245
- CVE-2017-9420
- CVE 2017-1000117

3 Avaliação

Tabela 1: Critérios de Avaliação

Critérios de Avaliação	**Pontos**
Explicação do serviço e da falha	2,0
Demonstração clara do problema no código-fonte do serviço	2,0
Apresentação e explicação do código-fonte do exploit que explora a vulnerabilidade	1,0
Apresentação da vulnerabilidade ao vivo	2,0
Apresentação e explicação do código-fonte do patch que corrige a vulnerabilidade	2,0
Demonstração de que com o patch a vulnerabilidade deixa de existir	1,0
Total	**10,0**

Perguntas serão feitas pelo professor após a apresentação a fim de definir as notas finais de cada um dos itens acima. **Não é necessário codificar um novo exploit e nem um novo patch para a vulnerabilidade. Vocês podem usar algo que já existe mas devem deixar claro quem são os autores.**

3.1 Punições

- **Escrita das informações na planilha disponível no PACA fora do prazo**: quem escrever as informações fora do prazo, mesmo que por 1 segundo, terá nota ZERO no EP.
- **Não apresentar o tópico para o professor**: quem não apresentar o tópico para o professor na sala de aula, antes de escrever na planilha no fórum da disciplina, terá nota ZERO no EP.
- **Divisão injusta na apresentação**: se durante a apresentação não houver uma divisão justa para cada um falar/demonstrar algo, a nota final do EP será a nota dada pelo professor dividida pela quantidade de integrantes da equipe.

4 Datas

- Escrita das informações na planilha disponível no PACA: **até 7/11 às 8:00**
- Dias para as apresentações (em cada dia poderá haver até 2 apresentações): **21/11, 26/11, 28/11, 3/12, e 5/12**.